

DOCKET FILE COPY ORIGINAL

**ENERGY MANAGEMENT ASSOCIATES**

*The Utilities Division of EDS*

RECEIVED

JAN 31 1994

FCC - MAIL ROOM

January 25, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company location communications system, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information services and equipment provided IXCs LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

When the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Spring Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service

No. of Copies rec'd  
LHM ABCDE

0-4

offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day. As hackers begin new methods of breaking into systems by using local ones instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the system and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in cursive script, reading "Dorothy L. Abass".

Dorothy L. Abass  
Administrative Coordinator



DO NOT FILE COPY ORIGINAL

January 28, 1994

Mr. William F. Caton  
Acting Secretary  
Federal Communications Commission  
Common Carrier Bureau  
1919 M. Street NW  
Washington, DC 20554

RECEIVED

JAN 31 1994

FCC - MAIL ROOM

Re: FCC Docket #93-292; Toll Fraud

Dear Mr. Caton,

As a large user of telecommunication services, it is our feeling that manufacturers of PBX equipment and adjunct devices (Voice Mail) must take more responsibility in prevention, detection and liability of toll fraud. It is our belief that manufacturers must alert customers to potential "gateways of fraud" and work with them to close these areas of access. This process should be included as part of any detailed implementation plan. If all avenues are checked and measures are taken to protect customer hardware and fraud still occurs, the manufacturer should at least share in the financial liability. Customer failure to implement suggested protective measures should place financial burden on the customer.

At present, it is our finding that "security" is not formally covered during system implementation unless initiated as a topic by the customer. This is totally irresponsible, considering the magnitude of the toll fraud problem. This again shows just cause for vendor liability. It has been our experience around the world, that more companies should place the same emphasis on toll fraud and security that the people of AT&T Network Security do in New Jersey. This organization has taken a completely proactive stand in fighting toll fraud (see attached letter from one of our divisions). Only through such aggressive measures as AT&T Security takes, can toll fraud be brought under control.

Sincerely,

Richard W. Gabler  
Director Telecommunications &  
Network Services  
Emerson Electric Co.

RWG/mi

Attachment

No. of Copies rec'd 0+4  
List ABCDE



Tekmar Company  
1145 East Kemper Road  
P.O. Box 428878  
Cincinnati, OH 45242-8878  
Tel: (513) 247-7200  
Sales (800) 543-4467  
Service (800) 874-2001  
Fax: (513) 247-7250 • Telex: 211 801

19 January 1994

Mr. Ralph Stanze  
AT&T  
424 South Woodsmill Road  
Chesterfield, Mo. 63017

RECEIVED

JAN 31 1994

REC-MAIL ROOM

Ralph,

I wanted to provide you some feedback on a recent phone fraud case that AT&T's Corporate security office detected for us. The first indication was unusual traffic to our 1-800-433-2341 during the nights of Jan 15 and 16th. Apparently someone had gotten into our phone system through the 800 number which is forwarded to voice mail / automated attendant after normal hours. They then gained access through the Audix integrated installation services voicemail package to initiate long distance calls. This was disturbing because we had disabled all outcalling through voice mail. Somehow they gained access to one of our 10 Cincinnati Bell local outbound trunks and initiated long distance calls to Gambia, and other places. (We have not yet received an invoice detailing these charges from Cincinnati Bell - the next billing cycle is 5 February.)

At&T Corporate security left us a message Sunday morning (16 January) at roughly 6:00am indicating that toll fraud was a distinct possibility because of the length of connect time and because the originating calls were from 3 residences and 1 coin phone in the 212 area code (Bronx, NY). The case number was PH 011 540 0017. AT&T Corporate Security then recommended that we contact their Denver office (1-800-628-2888) which has equipment specialists that can remotely assess our exposure to possible fraud, make changes to tighten security, and recommend changes that we can make to limit our exposure to toll fraud. This involved separate groups for hardware (SYSTEM 25) and "software" - Audix integrated installation services. The recommendations implemented were:

1. disable remote access for one of our ports.
2. change the option on transfer to another station within voice mail to only allow transfers to existing voice mail stations.

This second recommendation probably closed the outbound traffic. In addition, we requested that Cincinnati Bell block our 10 local trunks from using 3rd party billing and long distance. On Tuesday night and early morning Wednesday (18,19 January) we detected some activity through the call accounting software of several successive

attempts to connect with a duration of 1 minute or less - but no connect times of 1,2, or 3 hours as we saw the previous nights. We hope that the actions described above have ended this problem for TEKMAR. I will follow up with Rich Gabler and provide him details on charges when we get them from Cincinnati Bell. By the way, their recommended approach is apparently review the monthly invoice for usage and dispute incorrect charges - not a proactive method.

Additional recommendations we are implementing as a result of this include:

1. posting an instruction to all phone attendants that no unauthorized access be given to voice mail, or the phone system itself - even if the person claims to be with the phone company...
2. continue to monitor after hour usage for long connect times.
3. encourage people to frequently change voice mail passwords, and use passwords different from the station itself...
4. practice "safe" calling card use when using the AT&T calling cards - make sure no one is looking over your shoulder, cover card access number to prevent casual access, ...

I am writing this memo to express TEKMAR's gratitude for AT&T's timely detection of this problem. AT&T's prompt notification of the incident and pool of technical resources has helped to prevent a potentially significant loss due to toll fraud charges. Keep up the good work! - please pass this on to the Corporate Security group.

Without this timely notification, the problem quite honestly would have gone undetected until we received our monthly invoice from Cincinnati Bell. Even then, if the charges were "reasonable" in comparison to previous months it may have never been detected. The AT&T Call Accounting Software that we run internally on the SYSTEM 25 to review phone usage showed only a long connect time - but no outbound dialed numbers and no toll charges - again amplifying the fact that this episode would not have been detected. AT&T's proactive approach to quickly detect and notify clients of suspected fraud is a significant value added service.

Sincerely,

*Rich*  
Rich Beck  
MIS Manager TEKMAR  
(513)-247-7080

CC: ~~██████████~~ - Emerson Electric Co. St.Louis  
Don Harris, Ray Knueven, Jackie Kissing, Don Brown,  
Kris McCauley - TEKMAR

DO NOT WRITE IN THESE SPACES

JAN 31 1994

FCC - WASHINGTON



**Security  
Systems, Inc.**

January 10, 1993

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

300 Interpace Parkway  
Parsippany  
NJ 07054-1113  
Telephone 201 316 1000  
Telex 667729  
Fax 201 316 1131

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd  
List ABCDE

*Orig.*

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

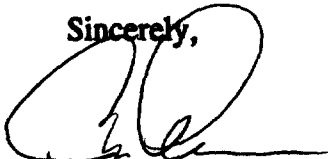
However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

A handwritten signature in black ink, appearing to be 'Ron Carr', written over a horizontal line.

Ron Carr  
Director, Corporate Telecommunications

Joseph T. Ryerson & Son, Inc.  
16th & Rockwell Streets, Chicago  
Mail Address: Box 8000  
Chicago, Illinois 60680

312 762 2121

RECEIVED

JAN 31 1994



**Ryerson**

FCC MAIL ROOM

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket 93-292

Dear Mr. Canton:

It was with great interest as I read the recent Federal Communications Commission (FCC) Notice of Proposed Rule Making Concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rule making. Whereas, I have taken each and every protective step recommended by the IXC and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud, if we do not control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, equipment and services provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs, who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords, which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not as an addition that you have to purchase later.

No. of Copies rec'd Orig.  
List ABCDE



Mr. William F. Canton

Page 2

While the programs offered by IXCs; such as MCI Detect, AT&T NetProtect and Sprint Guard, have broken new ground in relation to preventing toll fraud, they still do not do enough. Some of these services are too expensive for smaller companies and the education information is superficial. Monitoring by IXCs should be a part of the basic inter-exchange service offerings, since all companies (large and small) are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there would not be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking into systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXCs.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with the features and require IXCs and LECs to offer detection, prevention and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll occurs, then liability should be shared equally.


However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there would not be a toll fraud problem. While it is the hacker who breaks into the systems and sells the information, it is the "call sell" operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,



Eric P. Gilbert  
Manager  
Business Systems

**DREW ECKL & FARNHAM**

ATTORNEYS AT LAW

880 WEST PEACHTREE STREET

P.O. BOX 7600

ATLANTA, GEORGIA 30357-0600

(404) 885-1400

January 14, 1994

**RECEIVED****JAN 31 1994****FCC MAIL ROOM**

CHARLES L. DREW	DONALD R. ANDERSEN	MAUREEN M. MIDDLETON
W. WRAY ECKL	JOHN G. BLACKMON, JR.	ROBERT L. WELCH
CLAYTON H. FARNHAM	GARY R. HURST	JULIE Y. JOHN
ARTHUR H. GLASER	KEVIN P. O'MAHONY	JEFFREY B. GRIMM
JAMES M. POE	ANNE M. LANDRUM	KRISTEN K. DUGGAN
JOHN A. FERGUSON, JR.	NENA K. PUCKETT	SUZANNE V. SANDERS
THEODORE FREEMAN	MARI L. MYER	LEIGH LAWSON REEVES
JOHN P. REALE	JANE ROSS LEITZ	BONNIE M. WHARTON
STEVEN A. MILLER	NICOLE D. TIFVERMAN	RICHARD B. MILLER II
H. MICHAEL BAGLEY	JERRY C. CARTER, JR.	BRUCE A. TAYLOR, JR.
HALL F. MCKINLEY III	PHILLIP E. FRIDUSS	DOUGLAS T. LAY
G. RANDALL MOODY	L. LEE BENNETT, JR.	VIRGINIA A. GREEN
B. HOLLAND PRITCHARD	CHRISTOPHER J. CULP	DOUGLAS M. BAKER
T. BART GARY	SCOTT T. BUSHNELL	ELIZABETH B. LUZURIAGA
RICHARD T. GIERYN, JR.	KATHERINE D. DIXON	DAVID R. BERGQUIST
DAVID A. SMITH	WILLIAM T. MITCHELL	R. HAROLD MCCARD, JR.
KENNETH A. HINDMAN	J. ROBB CRUSER	CHARLES L. NORTON, JR.
PAUL W. BURKE	JENNIFER D. WELCH	MICHAEL J. CRIST
DANIEL C. KNIFFEN	PHILIP W. SAVRIN	NANCY F. RIGBY
JOHN C. BRUFFEY, JR.	LUCIAN GILLIS, JR.	LORI V. WINKLEMAN
BENTON J. MATHIS, JR.	PETER H. SCHMIDT II	PETER A. LAW
DENNIS M. HALL	BROOKS B. POWERS	DOUGLAS G. SMITH
J. WILLIAM HALEY	APRIL RICH	TERRANCE T. ROCK

FACSIMILE (404) 876-0992

WRITER'S DIRECT DIAL NUMBER

(404) 885-6242

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, D.C. 20554

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't

No. of Copies rec'd *Aug.*  
List ABCDE

Mr. William F. Canton  
RE: CC Docket 93-292  
January 14, 1994  
Page 2

RECEIVED  
JAN 31 1994  
FCC MAIL ROOM

knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXC's, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXC's should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXC's were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only 'hack' to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method for law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

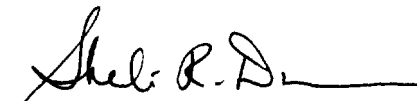
Mr. William F. Canton  
RE: CC Docket 93-292  
January 14, 1994  
Page 3

RECEIVED  
JAN 31 1994  
FCC MAIL ROOM

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

DREW ECKL & FARNHAM

  
Sheli R. Dunn  
Systems Manager

/srd

DO NOT FILE COPY ORIGINAL

RECEIVED

JAN 31 1994

FCC MAIL ROOM



# St. Anthony's Medical Center

January 25, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

RE: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard<sup>TM</sup>, MCI Detect<sup>TM</sup>, and AT&T Netprotect<sup>TM</sup>) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

Richard Grisham  
President and Chief  
Executive Officer

No. of Copies *orig*  
List ABOVE

Mr. William F. Canton  
January 25, 1994  
Page Two

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

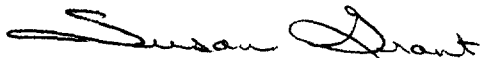
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXCs and LECs to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties, then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together, we can and will make a positive impact on this problem.

Sincerely,



Susan Grant, Supervisor  
Telecommunications

ph



University of Pittsburgh  
Medical Center

DOCKET FILE COPY ORIGINAL

RECEIVED



JAN 31 1994

DeSoto at O'Hara Streets  
Pittsburgh, PA 15213-2582

January 25, 1994

FCC MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

RE: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud, which occur over greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are just as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of approaching an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud as it specifically relates to their equipment and to provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor,

No. of Copies rec'd  
List ABCOE

*Aug*

should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software included in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will required clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendors, LEC's and IXC's involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Edward J. Miske, Manager  
ISD Voice Communications

/kw



January 11, 1994

**RECEIVED**

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

**JAN 31 1994**

**FCC MAIL ROOM**

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABCDE

*Orig.*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

  
Providence Telecom. Network

**City and County of San Francisco**



Office of the General Manager  
H. DANIEL McFARLAND

**DEPARTMENT OF ELECTRICITY  
AND TELECOMMUNICATIONS**

**RECEIVED**

DOCKET FILE COPY ORIGINAL

**JAN 31 1994**

901 Rankin Street  
San Francisco, California 94124  
(415) 550-2720

**FCC MAIL ROOM**

January 11, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for the City and County of San Francisco's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABOVE

*Orig.*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All logon IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment;
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment; and
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services.

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is not proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,



Carl A. Ruiz

Manager, Telecommunications Division

cc: H. D. McFarland  
F. Weiner

January 11, 1994

RECEIVED

JAN 31 1994

FCC MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

*Orig.*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

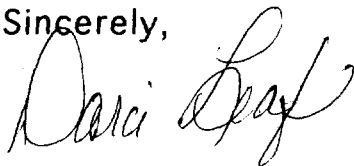
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in cursive script, appearing to read "Darci Gray".

January 11, 1994

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 31 1994

FCC MAIL ROOM

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd  
List ABOVE

*Orig.*

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

*Antoinette Asmus*  
Director, Telecommunications  
Good Samaritan Hospital  
375 Dix Mith Ave  
Cincinnati, Ohio 45220



DOCKET FILE COPY ORIGINAL

# The University of Kansas

RECEIVED

JAN 31 1994

FCC MAIL ROOM

Telecommunications Department

January 25, 1994

Mr. William F. Canton  
Acting Secretary  
Federal Communications Commission  
1919 M Street NW  
Washington, DC 20554

Re: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule-making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features, but also by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard<sup>TM</sup>, MCI Detect<sup>TM</sup>, and AT&T Netprotect<sup>TM</sup>) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPEs should be delivered without standard default passwords, which are well-known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer

No. of Copies rec'd  
LHM ABCDE  
DHC